日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　５月１１日

出願番号
Application Number: 特願２０００－１３８６４２

出願人
Applicant (s): 松下電器産業株式会社

２０００年１１月　６日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０９２０８１

【書類名】　特許願

【整理番号】　2022520200

【提出日】　平成12年 5月11日

【あて先】　特許庁長官殿

【国際特許分類】　G09C 1/00

G06F 12/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　松崎　なつめ

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　江村　里志

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　稲垣　悟

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　ファイル暗号装置、ファイル復号装置及びファイル暗号復号システム

【特許請求の範囲】

【請求項１】　パスワードと鍵情報を用いてファイルを暗号化する装置であって、パスワードの登録時に、前記鍵情報を入力パスワードで暗号化した暗号化鍵を装置内に保存し、ファイルと前記鍵情報を入力とし、任意に生成したファイル鍵を前記鍵情報を用いて暗号化した暗号化ファイル鍵と、前記ファイルを前記ファイル鍵を用いて暗号化した暗号化ファイルを出力するファイル暗号部を備え、前記暗号化ファイル鍵を前記暗号化ファイルのヘッダに格納して共に保存することを特徴としたファイル暗号装置。

【請求項２】　前記請求項１記載のファイル暗号装置からの出力を復号化するファイル復号化装置であって、ファイル暗号部で暗号化された前記ヘッダ付きの暗号化ファイルと、前記暗号化鍵と前記パスワード、あるいは前記鍵情報を入力とし、前記暗号化鍵を前記パスワードを用いて復号して前記鍵情報を取り出し、前記ヘッダより取り出した暗号化ファイル鍵を前記鍵情報で復号してファイル鍵を取り出し、前記暗号化ファイルを前記ファイル鍵で復号して取り出したファイルを出力するファイル復号部を備えたことを特徴としたファイル復号装置。

【請求項３】　パスワードの登録時に、前記鍵情報を入力パスワードで暗号化した暗号化鍵を装置内に保存し、ファイルと前記鍵情報を入力とし、任意に生成したファイル鍵を前記鍵情報を用いて暗号化した暗号化ファイル鍵と、前記ファイルを前記ファイル鍵を用いて暗号化した暗号化ファイルを出力するファイル暗号部を備え、前記暗号化ファイル鍵を前記暗号化ファイルのヘッダに格納して共に保存し、前記ファイル暗号部で暗号化された前記ヘッダ付きの暗号化ファイルと、前記暗号化鍵と前記パスワード、あるいは前記鍵情報を入力とし、前記暗号化鍵を前記パスワードを用いて復号して前記鍵情報を取り出し、前記ヘッダより取り出した暗号化ファイル鍵を前記鍵情報で復号してファイル鍵を取り出し、前記暗号化ファイルを前記ファイル鍵で復号して取り出したファイルを出力するファイル復号部を備えたことを特徴としたファイル暗号復号システム。

【請求項４】　前記暗号化鍵を、入力パスワードに対応したＩＤと対にして保存することを特徴とした請求項１記載のファイル暗号装置。

【請求項５】　前記暗号化鍵、あるいは前記鍵情報、あるいは入力ファイルの認証情報を、前記暗号化鍵あるいは暗号化ファイルヘッダに追加し、前記ファイル復号部において認証情報を確認することを特徴とした請求項３記載のファイル暗号復号システム。

【請求項６】　前記暗号化鍵を可搬媒体に保存して、前記ファイル復号部でパスワードと共に使用することを特徴とした請求項３記載のファイル暗号復号システム。

【請求項７】　パスワードの紛失時に、前記暗号化鍵を装置内から消去することを特徴とした請求項３記載のファイル暗号復号システム。

【請求項８】　パスワードの変更時に、前記鍵情報を新しい入力パスワードで暗号化した暗号化鍵を装置内に再設定することを特徴とした請求項１記載のファイル暗号装置。

【請求項９】　鍵情報の変更時に、前記暗号化鍵を前記パスワードを用いて復号して鍵情報を取り出し、前記ヘッダより取り出した暗号化ファイル鍵を前記鍵情報で復号してファイル鍵を取り出し、これを新しい鍵情報で暗号化してこれを新しい暗号化ファイル鍵として前記暗号化ファイルヘッダに再設定し、さらに新しい鍵情報を入力したパスワードで暗号化してこれを新しい暗号化鍵として更新することを特徴とした請求項３記載のファイル暗号復号システム。

【請求項１０】　前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、暗号化ファイルのヘッダに保存し、これらの情報を用いて前記鍵情報の変更時に、変更対象となる暗号化ファイルを検索して変更することを特徴とした請求項９記載のファイル暗号復号システム。

【請求項１１】　前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、一括ファイルに管理保存し、この情報を用いて前記鍵情報の変更時に、変更対象となる暗号化ファイルを検索して変更することを特徴とした請求項９記載のファイル暗号復号システム。

【請求項１２】　前記暗号化鍵を前記暗号化ファイルのヘッダに格納すること

を特徴とする請求項３記載のファイル暗号復号システム。

【請求項１３】　前記ファイル暗号部において、外部からの指示あるいはファイルの特性により、前記暗号化鍵を暗号化ファイルのヘッダに格納する、あるいは格納しないのいずれかを選択することを特徴とした請求項１２記載のファイル暗号装置。

【請求項１４】　前記暗号化鍵と鍵情報を同じ媒体に格納したことを特徴とする請求項１２記載のファイル暗号復号システム。

【請求項１５】　パスワードと鍵情報を用いてファイルを暗号化する装置であって、

パスワードの登録時に、入力パスワードを前記鍵情報で暗号化した暗号化パスワードを装置内に保存し、ファイルと前記鍵情報と前記暗号化パスワードを入力とし、前記鍵情報で前記暗号化パスワードを復号してパスワードを求め、任意に生成したファイル鍵を前記パスワードを用いて暗号化した第1の暗号化ファイル鍵と、前記ファイル鍵を前記鍵情報を用いて暗号化した第2の暗号化ファイル鍵と、前記ファイルを前記ファイル鍵を用いて暗号化した暗号化ファイルを出力するファイル暗号部を備え、前記第1、第2の暗号化ファイル鍵を前記暗号化ファイルのヘッダに格納して共に保存することを特徴とした、ファイル暗号装置。

【請求項１６】　前記請求項１５記載のファイル暗号装置からの出力を復号化するファイル復号装置であって、ファイル暗号部で暗号化された前記ヘッダ付きの暗号化ファイルと、前記パスワードあるいは前記鍵情報を入力とし、前記第1の暗号化鍵を前記パスワードを用いて復号して前記ファイル鍵を取り出し、あるいは前記第2の暗号化鍵を前記鍵情報を用いて復号して前記ファイル鍵を取り出し、前記暗号化ファイルを前記ファイル鍵で復号して取り出したファイルを出力するファイル復号部を備えたことを特徴としたファイル復号装置。

【請求項１７】　パスワードの登録時に、入力パスワードを前記鍵情報で暗号化した暗号化パスワードを装置内に保存し、ファイルと前記鍵情報と前記暗号化パスワードを入力とし、前記鍵情報で前記暗号化パスワードを復号してパスワードを求め、任意に生成したファイル鍵を前記パスワードを用いて暗号化した第1の暗号化ファイル鍵と、前記ファイル鍵を前記鍵情報を用いて暗号化した第2の

暗号化ファイル鍵と、前記ファイルを前記ファイル鍵を用いて暗号化した暗号化ファイルを出力するファイル暗号部を備え、前記第1、第2の暗号化ファイル鍵を前記暗号化ファイルのヘッダに格納して共に保存し、ファイル暗号部で暗号化された前記ヘッダ付きの暗号化ファイルと、前記パスワードあるいは前記鍵情報を入力とし、前記第1の暗号化鍵を前記パスワードを用いて復号して前記ファイル鍵を取り出し、あるいは前記第2の暗号化鍵を前記鍵情報を用いて復号して前記ファイル鍵を取り出し、前記暗号化ファイルを前記ファイル鍵で復号して取り出したファイルを出力するファイル復号部を備えたことを特徴としたファイル暗号復号システム。

【請求項１８】　前記暗号化パスワードを、入力パスワードと対応したＩＤと対にして保存することを特徴とした、請求項１５記載のファイル暗号装置。

【請求項１９】　前記ファイル暗号部において、外部からの指示あるいはファイルの特性により、前記第1の暗号化ファイル鍵を求める、あるいは求めないのいずれかを選択することを特徴とした、請求項１５記載のファイル暗号装置。

【請求項２０】　暗号化パスワードと鍵情報に認証子前記暗号化パスワードに認証情報を追加して前記ファイル暗号部で確認すること、あるいは前記鍵情報あるいは入力ファイルの認証情報を暗号化ファイルヘッダに追加し、前記ファイル復号部で確認することを特徴とした請求項１７記載のファイル暗号復号システム。

【請求項２１】　前記鍵情報と前記暗号化パスワードを同じ媒体に格納したことを特徴とした請求項１５記載のファイル暗号装置。

【請求項２２】　パスワードの紛失時またはパスワード変更時に、前記第２の暗号化鍵を前記鍵情報を用いて復号して前記ファイル鍵を取り出し、前記ファイル鍵を新しい入力パスワードで暗号化してこれを新しい第１の暗号化鍵として前記暗号化ファイルのヘッダに格納することを特徴とした請求項１７記載のファイル暗号復号システム。

【請求項２３】　鍵情報の紛失時に、前記第2の暗号化鍵を消去することを特徴とした請求項１７記載のファイル暗号復号システム。

【請求項２４】　鍵情報の変更時に、前記第１の暗号化鍵を前記パスワードを

用いて復号して前記ファイル鍵を取り出し、前記ファイル鍵を新しい鍵情報で暗号化してこれを新しい第２の暗号化鍵として前記暗号化ファイルのヘッダに格納することを特徴とした請求項１７記載のファイル暗号復号システム。

【請求項２５】　前記ファイル暗号部で暗号化された前記ヘッダ付きの暗号化ファイルと、前記パスワードおよび前記鍵情報を入力とし、前記第1の暗号化鍵を前記パスワードを用いて復号して前記ファイル鍵を取り出し、かつ前記第2の暗号化鍵を前記鍵情報を用いて復号して出力された結果を前記ファイル鍵と比較し、異なっているときにエラー処理をすることを特徴とした請求項１６記載のファイル復号装置。

【請求項２６】　前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、暗号化ファイルのヘッダに保存し、これらの情報を用いて前記パスワードの変更時に変更対象となる暗号化ファイルを検索して変更することを特徴とした請求項２２記載のファイル暗号復号システム。

【請求項２７】　前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、暗号化ファイルのヘッダに保存し、これらの情報を用いて前記鍵情報の変更時に変更対象となる暗号化ファイルを検索して変更することを特徴とした請求項２４記載のファイル暗号復号システム。

【請求項２８】　前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、一括ファイルに管理保存し、この情報を用いて前記パスワードの変更時に変更対象となる暗号化ファイルを検索して変更することを特徴とした、請求項２２記載のファイル暗号復号システム。

【請求項２９】　前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、一括ファイルに管理保存し、この情報を用いて前記鍵情報の変更時に変更対象となる暗号化ファイルを検索して変更することを特徴とした請求項２４記載のファイル暗号復号システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、計算機に付随した鍵情報を用いたファイルの暗号復号システムに関

する。特に、復号時に、予め登録されたパスワードだけでも復号できることを特徴とする。また、鍵情報やパスワードを紛失した際の、前の情報の無効化や更新の仕組みを備える。

【０００２】

【従来の技術】

従来のファイル暗号化装置として、例えば特許公開公報H09-204330に示されている方法がある。この方法においては、計算機内のファイルはある暗号鍵を用いて暗号化されて、特定の暗号情報格納領域に格納される。そして、特定のユーザがこの暗号情報格納領域にアクセスできるように、認証パスワードが登録されている。この仕組みにより、登録されている認証パスワードを入力すると、復号するための鍵が自動的に選ばれてファイルが復号できる。

【０００３】

しかしながら、この方法では、暗号化ファイルの安全性が、人間が記憶できるせいぜい数桁程度の認証パスワードのバラエティに帰着する。認証パスワードを用いるより、例えばICカードのような媒体に格納された（パスワードに比べて長いビット数の）鍵情報を用いて、ファイルの暗号および復号をするのが安全である。一方、暗号化されたファイルを別の装置に移動してそこで鍵情報がない緊急時には、パスワードだけでもファイルの復号を可能にする仕組みも必要とされる。また、パスワードを容易に変更できる仕組みも必要である。さらに、物理的な鍵情報を紛失した場合、悪意を持ったユーザの手に渡ったときのことも考え、再発行までの間、紛失した鍵情報を無効化して、さらに、すでに前の鍵情報を用いて暗号化された暗号化ファイルを、再発行された新しい鍵情報で復号できるようにする仕組みが必要である。

【０００４】

また、ファイルの暗号化のたびごとに、認証パスワードを入力する方法もあるが、入力が面倒でありまた、入力間違えもありうる。そのため一旦パスワードを登録しその後はパスワードの入力が不要であるほうが望ましい。また、登録したパスワードは安全に保管されなければならない。

【０００５】

【発明が解決しようとする課題】

上記従来の課題を解決するために、本発明では次の条件を満たすファイル暗号復号システムを提供することを目的とする。

【０００６】

(1)ICカードのような媒体に格納した鍵情報を用いてファイルの暗号化を行なう。パスワードはあらかじめ登録しておき、逐一のパスワード入力は必要ないものとする。

【０００７】

(2)前記鍵情報を用いてファイルの復号ができる。また、暗号化したときの指定によりあらかじめ登録したパスワードを用いたファイルの復号も可能とする。

【０００８】

(3)パスワードを容易に変更できる仕組みを備える。

【０００９】

(4)前記鍵情報を紛失した場合に、一時的に鍵情報を無効化する仕組みを備える。さらに、新しい鍵情報が再発行された場合に、新しい鍵情報で以前のファイルが取り扱えるための仕組みを備える。また、そのために変更すべき暗号化ファイルを自動的に検索する仕組みを備える。

【００１０】

【課題を解決するための手段】

本発明は、パスワードと鍵情報を用いてファイルを暗号化する装置であって、パスワードの登録時に、前記鍵情報を入力パスワードで暗号化した暗号化鍵を装置内に保存し、ファイルと前記鍵情報を入力とし、任意に生成したファイル鍵を前記鍵情報を用いて暗号化した暗号化ファイル鍵と、前記ファイルを前記ファイル鍵を用いて暗号化した暗号化ファイルを出力するファイル暗号部を備え、前記暗号化ファイル鍵を前記暗号化ファイルのヘッダに格納して共に保存することを特徴としたファイル暗号装置である。

【００１１】

また、本発明は、ファイル暗号部で暗号化された前記ヘッダ付きの暗号化ファイルと、前記暗号化鍵と前記パスワード、あるいは前記鍵情報を入力とし、前記

暗号化鍵を前記パスワードを用いて復号して前記鍵情報を取り出し、前記ヘッダより取り出した暗号化ファイル鍵を前記鍵情報で復号してファイル鍵を取り出し、前記暗号化ファイルを前記ファイル鍵で復号して取り出したファイルを出力するファイル復号部を備えたことを特徴としたファイル復号装置である。

【００１２】

また、本発明は、パスワードの登録時に、前記鍵情報を入力パスワードで暗号化した暗号化鍵を装置内に保存し、ファイルと前記鍵情報を入力とし、任意に生成したファイル鍵を前記鍵情報を用いて暗号化した暗号化ファイル鍵と、前記ファイルを前記ファイル鍵を用いて暗号化した暗号化ファイルを出力するファイル暗号部を備え、前記暗号化ファイル鍵を前記暗号化ファイルのヘッダに格納して共に保存し、前記ファイル暗号部で暗号化された前記ヘッダ付きの暗号化ファイルと、前記暗号化鍵と前記パスワード、あるいは前記鍵情報を入力とし、前記暗号化鍵を前記パスワードを用いて復号して前記鍵情報を取り出し、前記ヘッダより取り出した暗号化ファイル鍵を前記鍵情報で復号してファイル鍵を取り出し、前記暗号化ファイルを前記ファイル鍵で復号して取り出したファイルを出力するファイル復号部を備えたことを特徴としたファイル暗号復号システムである。

【００１３】

また、本発明は、前記暗号化鍵を、入力パスワードに対応したＩＤと対にして保存することを特徴としたファイル暗号装置である。

【００１４】

また、本発明は、前記暗号化鍵、あるいは前記鍵情報、あるいは入力ファイルの認証情報を、前記暗号化鍵あるいは暗号化ファイルヘッダに追加し、前記ファイル復号部において認証情報を確認することを特徴としたファイル暗号復号システムである。

【００１５】

また、本発明は、前記暗号化鍵を可搬媒体に保存して、前記ファイル復号部でパスワードと共に使用することを特徴としたファイル暗号復号システムである。

【００１６】

また、本発明は、パスワードの紛失時に、前記暗号化鍵を装置内から消去する

ことを特徴としたファイル暗号復号システムである。

【００１７】

また、本発明は、パスワードの変更時に、前記鍵情報を新しい入力パスワードで暗号化した暗号化鍵を装置内に再設定することを特徴としたファイル暗号装置である。

【００１８】

また、本発明は、鍵情報の変更時に、前記暗号化鍵を前記パスワードを用いて復号して鍵情報を取り出し、前記ヘッダより取り出した暗号化ファイル鍵を前記鍵情報で復号してファイル鍵を取り出し、これを新しい鍵情報で暗号化してこれを新しい暗号化ファイル鍵として前記暗号化ファイルヘッダに再設定し、さらに新しい鍵情報を入力したパスワードで暗号化してこれを新しい暗号化鍵として更新することを特徴としたファイル暗号復号システムである。

【００１９】

また、本発明は、前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、暗号化ファイルのヘッダに保存し、これらの情報を用いて前記鍵情報の変更時に、変更対象となる暗号化ファイルを検索して変更することを特徴としたファイル暗号復号システムである。

【００２０】

また、本発明は、前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、一括ファイルに管理保存し、この情報を用いて前記鍵情報の変更時に、変更対象となる暗号化ファイルを検索して変更することを特徴としたファイル暗号復号システムである。

【００２１】

また、本発明は、前記暗号化鍵を前記暗号化ファイルのヘッダに格納することを特徴とするファイル暗号復号システムである。

【００２２】

また、本発明は、前記ファイル暗号部において、外部からの指示あるいはファイルの特性により、前記暗号化鍵を暗号化ファイルのヘッダに格納する、あるいは格納しないのいずれかを選択することを特徴としたファイル暗号装置である。

【００２３】

また、本発明は、前記暗号化鍵と鍵情報を同じ媒体に格納したことを特徴とするファイル暗号復号システムである。

【００２４】

また、本発明は、パスワードと鍵情報を用いてファイルを暗号化する装置であって、パスワードの登録時に、入力パスワードを前記鍵情報で暗号化した暗号化パスワードを装置内に保存し、ファイルと前記鍵情報と前記暗号化パスワードを入力とし、前記鍵情報で前記暗号化パスワードを復号してパスワードを求め、任意に生成したファイル鍵を前記パスワードを用いて暗号化した第1の暗号化ファイル鍵と、前記ファイル鍵を前記鍵情報を用いて暗号化した第2の暗号化ファイル鍵と、前記ファイルを前記ファイル鍵を用いて暗号化した暗号化ファイルを出力するファイル暗号部を備え、前記第1、第2の暗号化ファイル鍵を前記暗号化ファイルのヘッダに格納して共に保存することを特徴とした、ファイル暗号装置である。

【００２５】

また、本発明は、ファイル暗号装置からの出力を復号化するファイル復号装置であって、ファイル暗号部で暗号化された前記ヘッダ付きの暗号化ファイルと、前記パスワードあるいは前記鍵情報を入力とし、前記第1の暗号化鍵を前記パスワードを用いて復号して前記ファイル鍵を取り出し、あるいは前記第2の暗号化鍵を前記鍵情報を用いて復号して前記ファイル鍵を取り出し、前記暗号化ファイルを前記ファイル鍵で復号して取り出したファイルを出力するファイル復号部を備えたことを特徴としたファイル復号装置である。

【００２６】

また、本発明は、パスワードの登録時に、入力パスワードを前記鍵情報で暗号化した暗号化パスワードを装置内に保存し、ファイルと前記鍵情報と前記暗号化パスワードを入力とし、前記鍵情報で前記暗号化パスワードを復号してパスワードを求め、任意に生成したファイル鍵を前記パスワードを用いて暗号化した第1の暗号化ファイル鍵と、前記ファイル鍵を前記鍵情報を用いて暗号化した第2の暗号化ファイル鍵と、前記ファイルを前記ファイル鍵を用いて暗号化した暗号化

ファイルを出力するファイル暗号部を備え、前記第1、第2の暗号化ファイル鍵を前記暗号化ファイルのヘッダに格納して共に保存し、ファイル暗号部で暗号化された前記ヘッダ付きの暗号化ファイルと、前記パスワードあるいは前記鍵情報を入力とし、前記第1の暗号化鍵を前記パスワードを用いて復号して前記ファイル鍵を取り出し、あるいは前記第2の暗号化鍵を前記鍵情報を用いて復号して前記ファイル鍵を取り出し、前記暗号化ファイルを前記ファイル鍵で復号して取り出したファイルを出力するファイル復号部を備えたことを特徴としたファイル暗号復号システムである。

【００２７】

また、本発明は、前記暗号化パスワードを、入力パスワードと対応したＩＤと対にして保存することを特徴としたファイル暗号装置である。

【００２８】

また、本発明は、前記ファイル暗号部において、外部からの指示あるいはファイルの特性により、暗号化ファイル鍵を求める、あるいは求めないのいずれかを選択することを特徴としたファイル暗号装置である。

【００２９】

また、本発明は、暗号化パスワードと鍵情報に認証子前記暗号化パスワードに認証情報を追加して前記ファイル暗号部で確認すること、あるいは前記鍵情報あるいは入力ファイルの認証情報を暗号化ファイルヘッダに追加し、前記ファイル復号部で確認することを特徴としたファイル暗号復号システムである。

【００３０】

また、本発明は、前記鍵情報と前記暗号化パスワードを同じ媒体に格納したことを特徴としたファイル暗号装置である。

【００３１】

また、本発明は、パスワードの紛失時またはパスワード変更時に、前記第２の暗号化鍵を前記鍵情報を用いて復号して前記ファイル鍵を取り出し、前記ファイル鍵を新しい入力パスワードで暗号化してこれを新しい第１の暗号化鍵として前記暗号化ファイルのヘッダに格納することを特徴としたファイル暗号復号システムである。

【００３２】

また、本発明は、鍵情報の紛失時に、前記第2の暗号化鍵を消去することを特徴としたファイル暗号復号システムである。

【００３３】

また、本発明は、鍵情報の変更時に、前記第１の暗号化鍵を前記パスワードを用いて復号して前記ファイル鍵を取り出し、前記ファイル鍵を新しい鍵情報で暗号化してこれを新しい第２の暗号化鍵として前記暗号化ファイルのヘッダに格納することを特徴としたファイル暗号復号システムである。

【００３４】

また、本発明は、前記ファイル暗号部で暗号化された前記ヘッダ付きの暗号化ファイルと、前記パスワードおよび前記鍵情報を入力とし、前記第1の暗号化鍵を前記パスワードを用いて復号して前記ファイル鍵を取り出し、かつ前記第2の暗号化鍵を前記鍵情報を用いて復号して出力された結果を前記ファイル鍵と比較し、異なっているときにエラー処理をすることを特徴としたファイル復号装置である。

【００３５】

また、本発明は、前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、暗号化ファイルのヘッダに保存し、これらの情報を用いて前記パスワードの変更時に変更対象となる暗号化ファイルを検索して変更することを特徴としたファイル暗号復号システムである。

【００３６】

また、本発明は、前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、暗号化ファイルのヘッダに保存し、これらの情報を用いて前記鍵情報の変更時に変更対象となる暗号化ファイルを検索して変更することを特徴としたファイル暗号復号システムである。

【００３７】

また、本発明は、前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、一括ファイルに管理保存し、この情報を用いて前記パスワードの変更時に変更対象となる暗号化ファイルを検索して変更することを特徴とした

ファイル暗号復号システムである。

【００３８】

また、本発明は、前記暗号化ファイルの暗号化の有無や、入力パスワードに対応したID情報を、一括ファイルに管理保存し、この情報を用いて前記鍵情報の変更時に変更対象となる暗号化ファイルを検索して変更することを特徴としたファイル暗号復号システムである。

【００３９】

【発明の実施の形態】

（実施形態１）

図１～図３に本発明の第1の実施の形態を示す。第1の実施の形態は、

(a)パスワードの登録：図１

(b)ファイルの暗号：図２

(c)暗号化ファイルの復号：図３

の３つの部分からなる。それぞれについて以下図に基づいて説明をする。なお、図中でEおよびDはそれぞれ暗号、復号の処理を示しており、任意の秘密鍵暗号を用いるものとする。またICカードのような媒体に鍵情報が格納されており、計算機本体に対応しているものとする。

【００４０】

まず、パスワードの登録時（図１）には、ユーザは鍵情報を設定しつつ登録するパスワードを入力する。パスワード登録部は、入力パスワードで鍵情報を暗号化し、その結果の暗号化鍵を計算機内に生成する。これはファイルとして保存して良い。

【００４１】

次にファイルの暗号時（図２）には、ユーザは鍵情報を設定しつつ暗号化するファイルを指定する。ファイル暗号部は、まず任意にファイル鍵を生成し、鍵情報でファイル鍵を暗号化して暗号化ファイル鍵を生成する。また、ファイル鍵でファイルの情報を暗号化して暗号化ファイルを生成する。そして暗号化ファイル鍵をヘッダにして、暗号化ファイルと共に保存する。

【００４２】

暗号化ファイルの復号には2つの方法がある。図３－１に示したのは、鍵情報を設定して暗号化ファイルを復号する方法である。このとき、暗号化ファイルのヘッダから獲得した暗号化ファイル鍵を鍵情報を用いて復号し、ファイル鍵を求める。そして、暗号化ファイルをそのファイル鍵で復号する。また図３－２に示したのは前記暗号化鍵とパスワードを用いて暗号化ファイルを復号する方法である。このとき、暗号化鍵をパスワードで復号し、鍵情報を求め、さらに鍵情報で暗号化ファイル鍵を復号してファイル鍵を求める。最後にファイル鍵で暗号化ファイルを復号してもとのファイル本体を求める。

【００４３】

なお、第1の実施の形態の次の事項も本発明の範囲である。

【００４４】

(1)暗号化鍵は特定の計算機の中にユーザIDと対応させて保存しておいても良い。

【００４５】

(2)パスワードを変更した場合には、暗号化鍵を更新するだけでよい。

【００４６】

(3)もしパスワードによる復号を禁止するためには、暗号化鍵を削除するだけで良い。

【００４７】

(4)鍵情報が更新されたときには暗号化鍵とパスワードを用いて更新前の鍵情報を一旦求めて、これでヘッダにある暗号化ファイル鍵を復号してファイル鍵を求める。その後新しい鍵情報でファイル鍵を暗号化して、暗号化ファイル鍵を更新する。また暗号化鍵も更新する必要がある。ただし、鍵情報を紛失しこれを一時的に無効化することはできない。

【００４８】

(5)ファイルの暗号時に暗号化ファイルのヘッダに暗号化の有無や対応する鍵情報のID情報を格納し、この情報を用いて、鍵情報が更新されたときに上記(4)の手順で変更すべき暗号化ファイルを検索すると便利である。また、各暗号化ファイルのヘッダの代わりに、この情報を一括してファイルに管理しておいても良

い。

【００４９】

(6)暗号化鍵はある計算機の中に保存しているものとしているため、パスワードによる復号は当該計算機でのみ可能となる。他の計算機においてパスワードによる復号を可能にするためには、暗号化鍵を何らかの別媒体に格納して他の計算機に入力する必要がある。

【００５０】

（実施形態２）

第2の実施の形態では、第1の実施の形態における暗号化鍵を、各暗号化ファイルのヘッダに暗号化ファイル鍵を共に格納する。図４にファイル暗号部、図５にパスワードを用いたファイル復号部の構成を示す。暗号化鍵をファイルのヘッダに格納することにより、（ヘッダ付きの）暗号化ファイルをそのまま他の計算機に移動して、パスワードだけで復号ができる。ただし、パスワードを変更した場合には、対応するファイルのヘッダ内の暗号化鍵をすべて更新する必要がある。また、ファイル暗号時に、必要となる暗号化鍵と鍵情報を同一の媒体に格納しておくと便利である。また、第2の実施の形態では、ファイルの暗号時に暗号化ファイルのヘッダに暗号化鍵を格納するかどうかを選択してもよい。暗号化鍵を格納しないファイルは、暗号化鍵を別途保持していない環境において、パスワードを用いたファイル復号ができない。

【００５１】

（実施形態３）

第3の実施の形態では、第1、第2の実施の形態で不可能であった、鍵情報を紛失したときの当該鍵情報の一時無効化を可能にする。以下、 図６～図８を参照しながら第3の実施の形態を説明する。第1の実施の形態と同様、第3の実施の形態も、

(a)パスワードの登録：図６

(b)ファイルの暗号：図７

(c)暗号化ファイルの復号：図８

の３つの部分からなる。それぞれについて図に基づいて説明をする。

【００５２】

まず、パスワードの登録時（図６）には、ユーザは鍵情報を設定しつつ登録するパスワードを入力する。パスワード登録部は、鍵情報で入力パスワードを暗号化し、その結果の暗号化パスワードを計算機内に生成する。第1、第2の実施の形態の暗号化鍵と鍵と情報が逆になっている。暗号化パスワードはファイルとして保存してよい。

【００５３】

次にファイルの暗号時（図７）には、ユーザは前記暗号化パスワードの存在する計算機において鍵情報を設定しつつ暗号化するファイルを指定する。ファイル暗号部は、まず前記暗号化パスワードを鍵情報で復号して、パスワードを求める。そして、任意に生成したファイル鍵をこのパスワードで暗号化して第１の暗号化ファイル鍵を生成する。また、鍵情報でファイル鍵を暗号化して第２の暗号化ファイル鍵を生成する。さらにファイル鍵でファイルの情報を暗号化して暗号化ファイルを生成する。そして第1、第2の暗号化ファイル鍵をヘッダにして、暗号化ファイルを保存する。

【００５４】

暗号化ファイルの復号には2つの方法がある。図８－１に示したのは、鍵情報を設定して暗号化ファイルを復号する方法である。このとき、暗号化ファイルのヘッダから獲得した第２の暗号化ファイル鍵を鍵情報で復号し、ファイル鍵を求める。そして、暗号化ファイルをそのファイル鍵で復号する。また図８－２に示したのはパスワードを用いて暗号化ファイルを復号する方法である。このとき、第１の暗号化鍵をパスワードで復号し、ファイル鍵を求める。そして暗号化ファイルをそのファイル鍵で復号してもとのファイル本体を求める。

【００５５】

なお、第３の実施の形態の次の事項も本発明の範囲である。

【００５６】

(1)暗号化パスワードは特定の計算機の中にユーザIDと対応させて保存しておいても良い。

【００５７】

(2)パスワードを変更した場合には、鍵情報を用いて第2の暗号化ファイル鍵を復号しファイル鍵を求める。そして、求めたファイル鍵を新しいパスワードを用いて暗号化して、これを第1の暗号化ファイル鍵として更新すれば良い。図９に手順を示す。

【００５８】

(3)もしパスワードによる復号を禁止するためには、第1の暗号化ファイル鍵を削除するだけで良い。このとき、鍵情報を用いたファイル復号は可能である。

【００５９】

(4)鍵情報を更新した場合には、パスワードを用いて第1の暗号化ファイル鍵を復号しファイル鍵を求める。そして、求めたファイル鍵を新しい鍵情報を用いて暗号化して、これを第2の暗号化ファイル鍵として更新すれば良い。図１０に手順を示す。

【００６０】

(5)もし鍵情報による復号を禁止するためには、第2の暗号化ファイル鍵を削除するだけでよい。このとき、パスワードを用いたファイル復号は可能である。

【００６１】

(6)暗号化鍵はある計算機の中に保存しているものとしているため、ファイル暗号化は当該計算機でのみ可能となる。他の計算機においてファイル暗号化を可能にするためには、暗号化パスワードを何らかの別媒体に格納して他の計算機に入力する必要がある。鍵情報と暗号化パスワードを同じ媒体に格納すると便利である。

【００６２】

(7)ファイルの暗号時に暗号化ファイルのヘッダに暗号化の有無や対応する鍵情報のID情報を格納し、この情報を用いて、鍵情報やパスワードが更新されたときに上記(2)または(4)の手順で変更すべき暗号化ファイルを検索すると便利である。また、各暗号化ファイルのヘッダの代わりに、この情報を一括してファイルに管理しておいても良い。

【００６３】

(8)ファイルの暗号時に、暗号化ファイルのヘッダに第1の暗号化ファイル鍵を

格納するかどうかを選択するようにしてもよい。格納するとパスワードによる暗号化ファイルの復号が可能になり、格納しないとパスワードによる復号が禁止できる。

【００６４】

上記(4)(5)の特徴により、ユーザが鍵情報を紛失した場合に、不正者が紛失した鍵情報を入手して復号することを禁止できる。ただし、パスワードによる復号は可能なので、新しい鍵情報が発行されるまでユーザ本人は不自由なくファイルをアクセスできる。また新しい鍵情報が再発行された場合には、暗号化ファイルヘッダを更新するだけで、新しい鍵情報で以降は復号できるようにできる。

【００６５】

なお、第3の実施の形態では、復号時に鍵情報とパスワードを両方要求するようにも設定できる。このとき、第1、第2の暗号化ファイル鍵をそれぞれで復号し、出力されたファイル鍵を双方比較することにより、ヘッダ部分の改ざんを検出することができる。

【００６６】

また、以上の第1から第3の実施の形態において、使用する暗号化鍵、暗号化パスワード、暗号化ファイル鍵等に、認証情報を付加してもよい。認証情報を付加することにより、実際にファイルを復号する前に、改ざんを検出することができる。

【００６７】

【発明の効果】

以上のように本発明によれば、計算機に付随した鍵情報を用いたファイルの暗号化と復号が可能になる。加えて、暗号時に指定すれば復号時に鍵情報無しで、あらかじめ登録して計算機内に安全に保管しておいたパスワードでも復号が可能になる。ファイル暗号時には逐次パスワードを設定する必要はない。また、パスワードを忘却したときにパスワードによる復号を一時的に無効化したり、新しいパスワードに容易に変更できる仕組みを備える。さらに、鍵情報を紛失したときに、鍵情報を一時的に無効化したり、新しい鍵情報が発行されたときにも、ヘッダだけを更新することにより、新しい鍵情報で前の鍵情報で暗号化したファイル

を扱えるための仕組みを備える。また、鍵情報やパスワードのIDをヘッダや一括管理ファイルに格納することにより、鍵情報やパスワードの変更時にそれに伴う変更が可能である暗号化ファイルを検索することができる。

【図面の簡単な説明】

【図１】

第1の実施の形態におけるパスワード登録の概要を示す図

【図２】

第1の実施の形態におけるファイル暗号を示す図

【図３】

第1の実施の形態における鍵情報またはパスワードを用いたファイル復号を示す図

【図４】

第2の実施の形態におけるファイル暗号を示す図

【図５】

第2の実施の形態におけるパスワードを用いたファイル復号を示す図

【図６】

第３の実施の形態におけるパスワード登録を示す図

【図７】

第３の実施の形態におけるファイル暗号を示す図

【図８】

第３の実施の形態における鍵情報またはパスワードを用いたファイル復号を示す図

【図９】

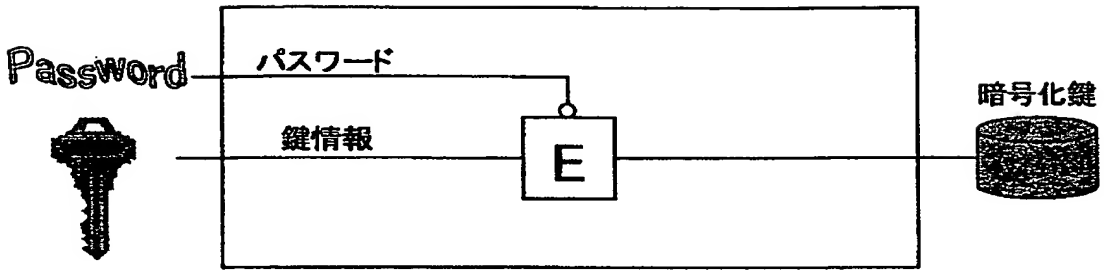
第3の実施の形態における、パスワードの無効化と更新を示す図

【図１０】

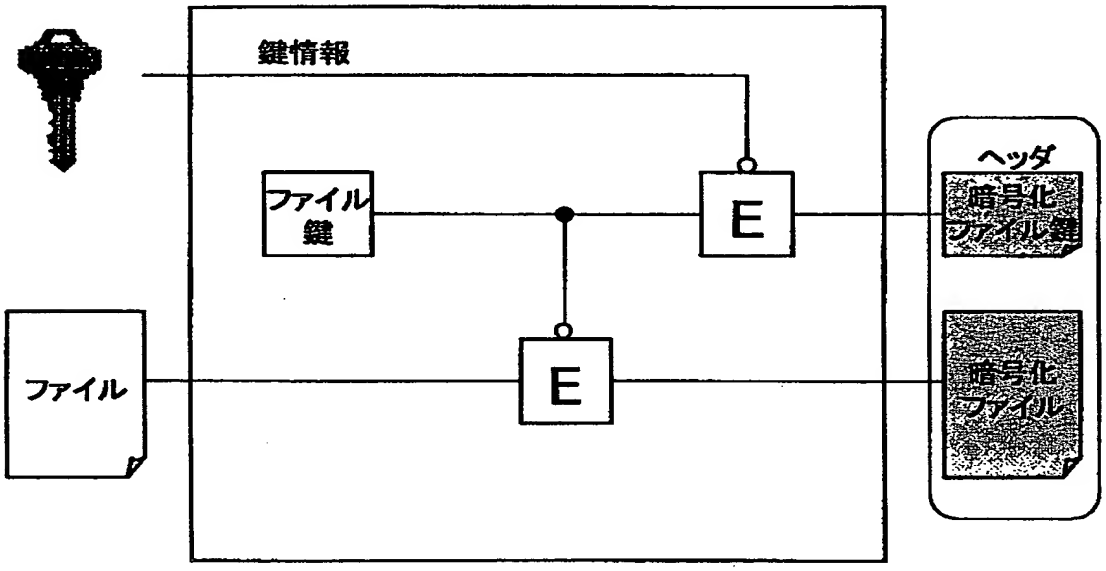
第3の実施の形態における、鍵情報の無効化と更新を示す図

【書類名】　　図面

【図１】

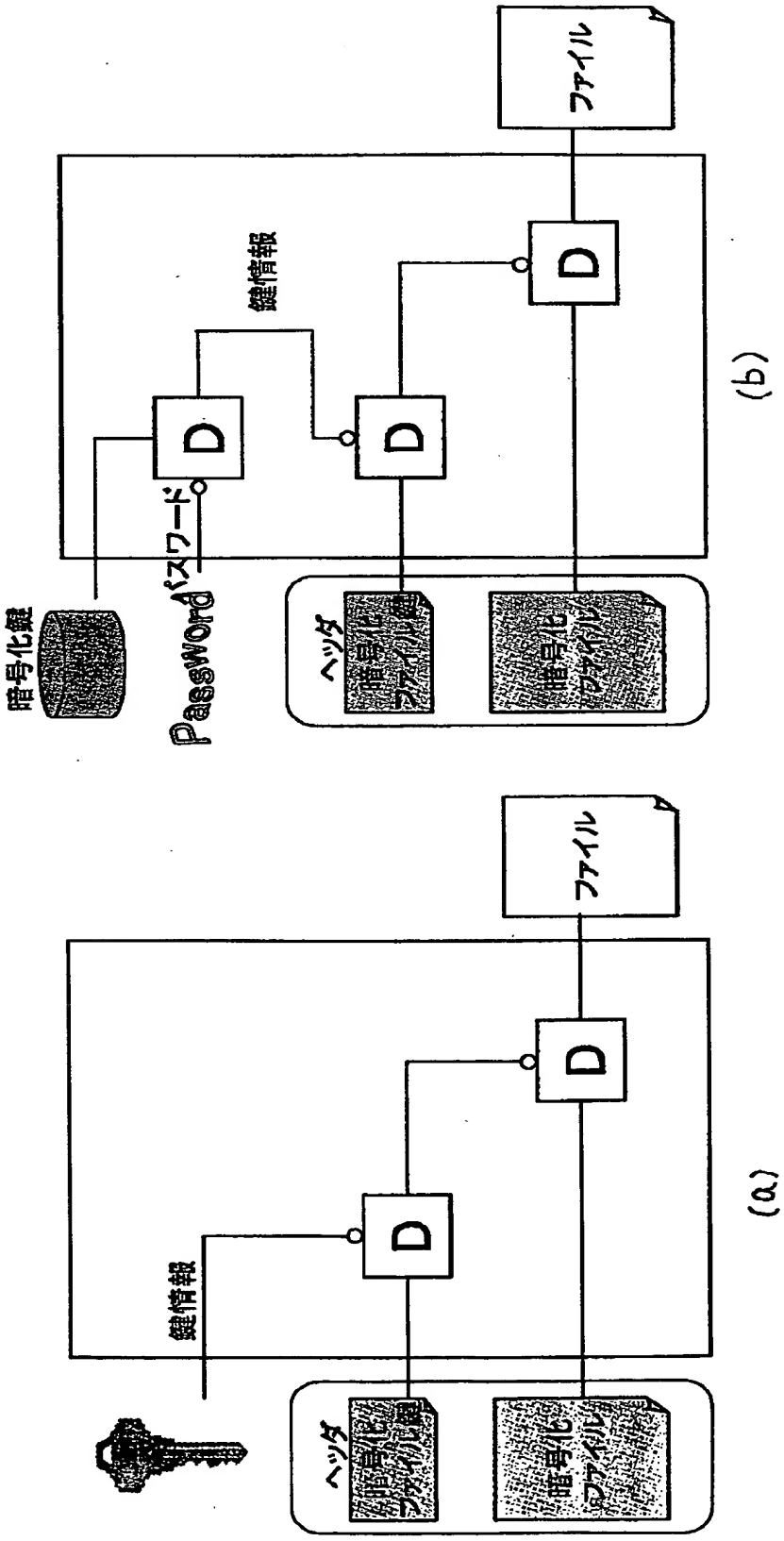


【図２】

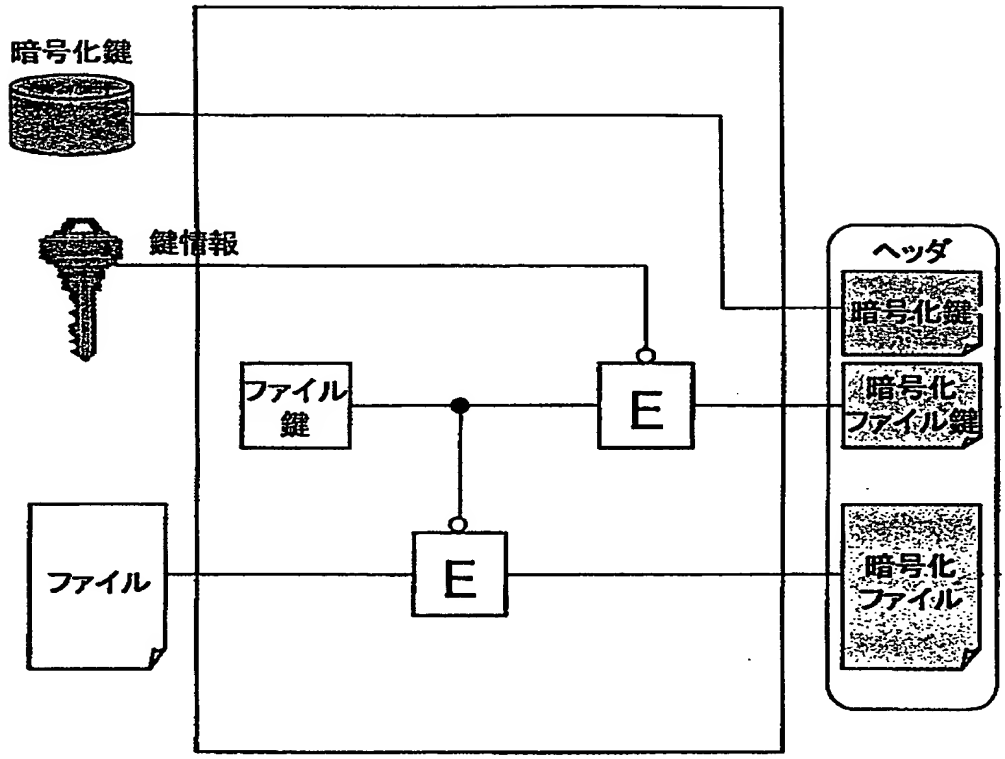


出証特２０００－３０９２０８１

【図３】

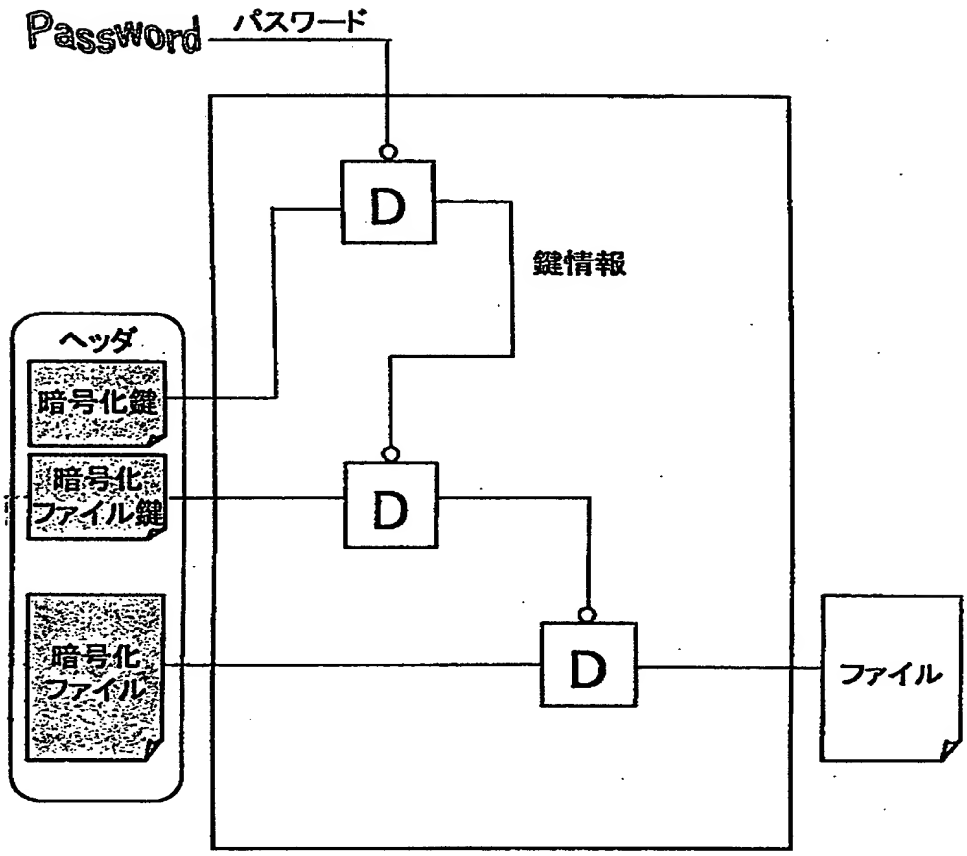

(a)
ファイル
D
D
鍵情報
ヘッダ
暗号化ファイル鍵
暗号化ファイル
(b)
ファイル
D
D
D
鍵情報
パスワード
Password
暗号化鍵
ヘッダ
暗号化ファイル鍵
暗号化ファイル

【図４】

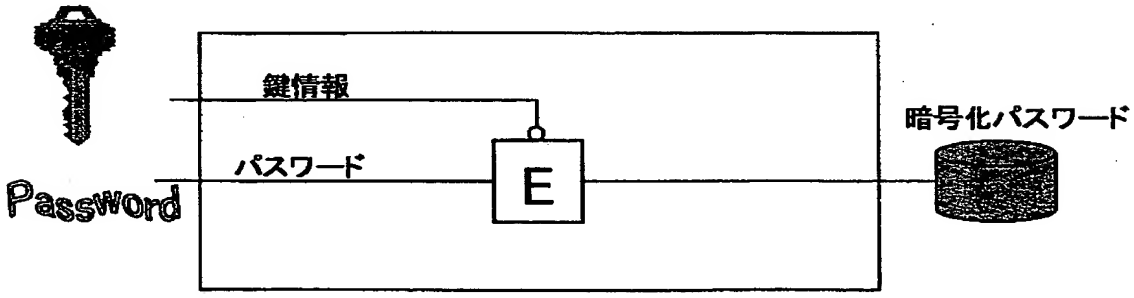


出証特２０００－３０９２０８１

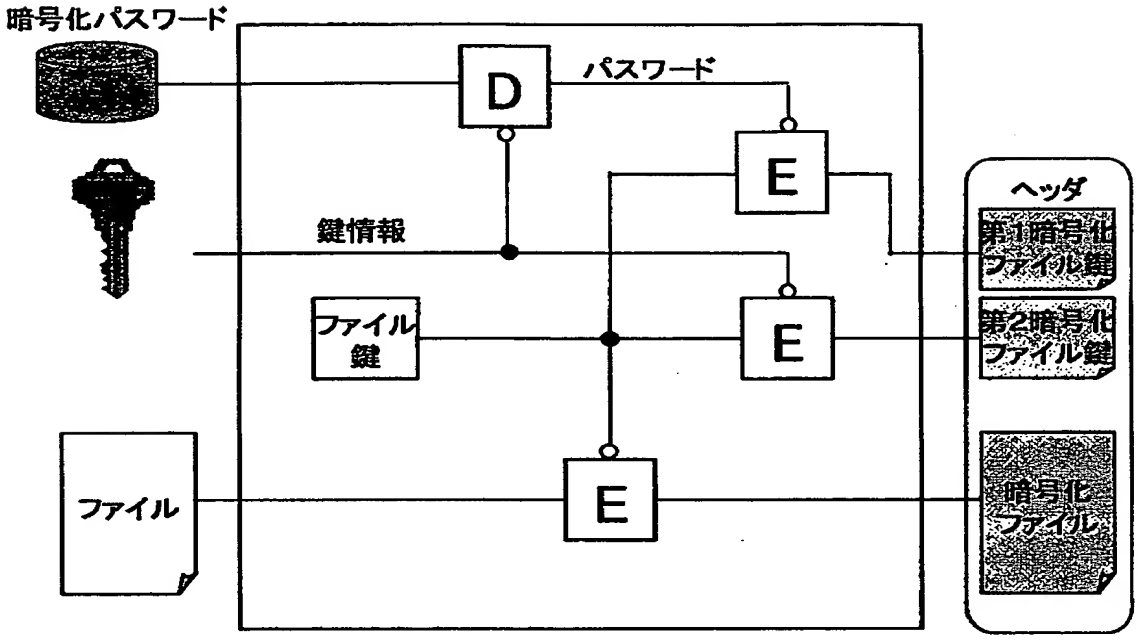
【図５】


Password
パスワード
D
鍵情報
ヘッダ
暗号化鍵
暗号化ファイル鍵
D
暗号化ファイル
D
ファイル

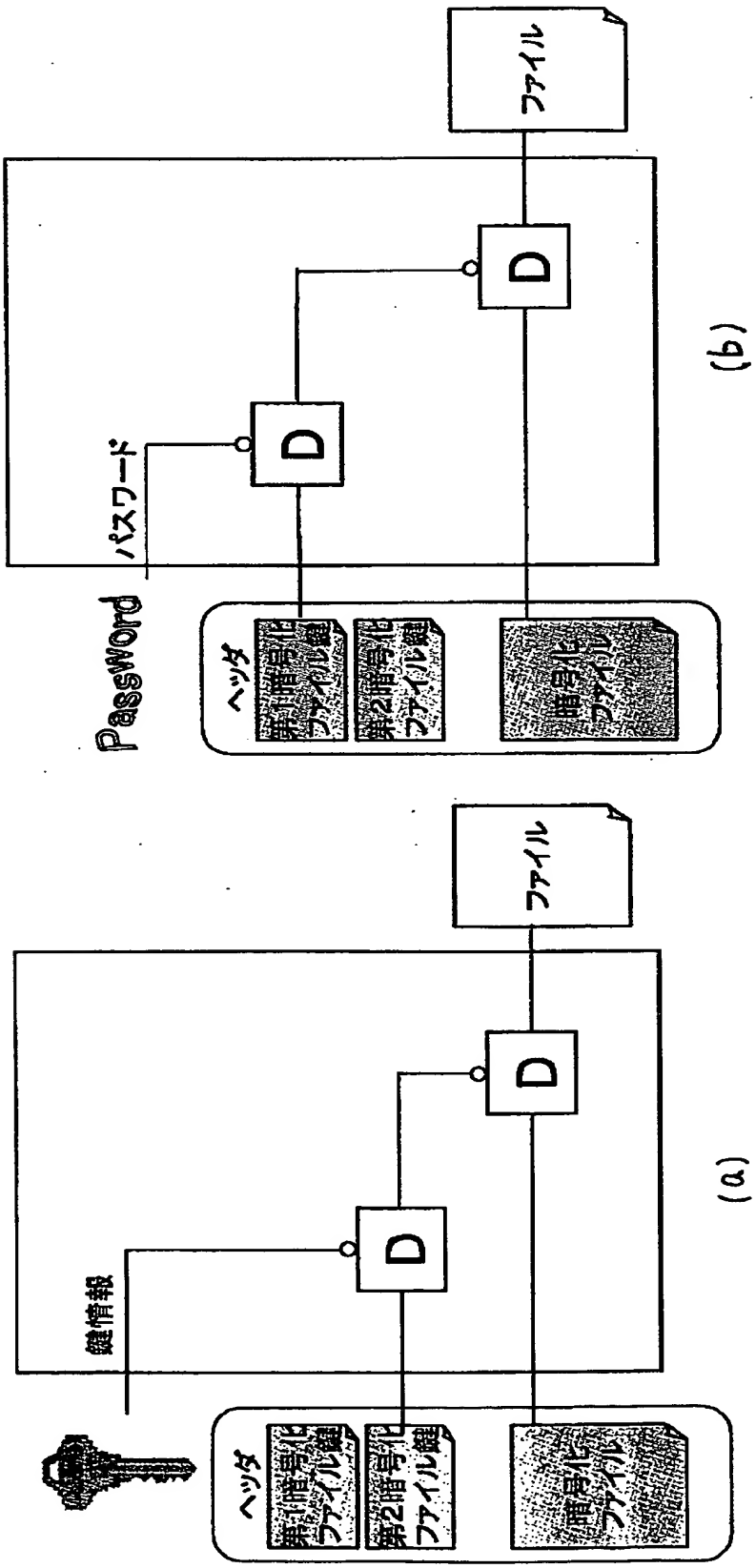
【図６】


鍵情報
パスワード
Password
E
暗号化パスワード

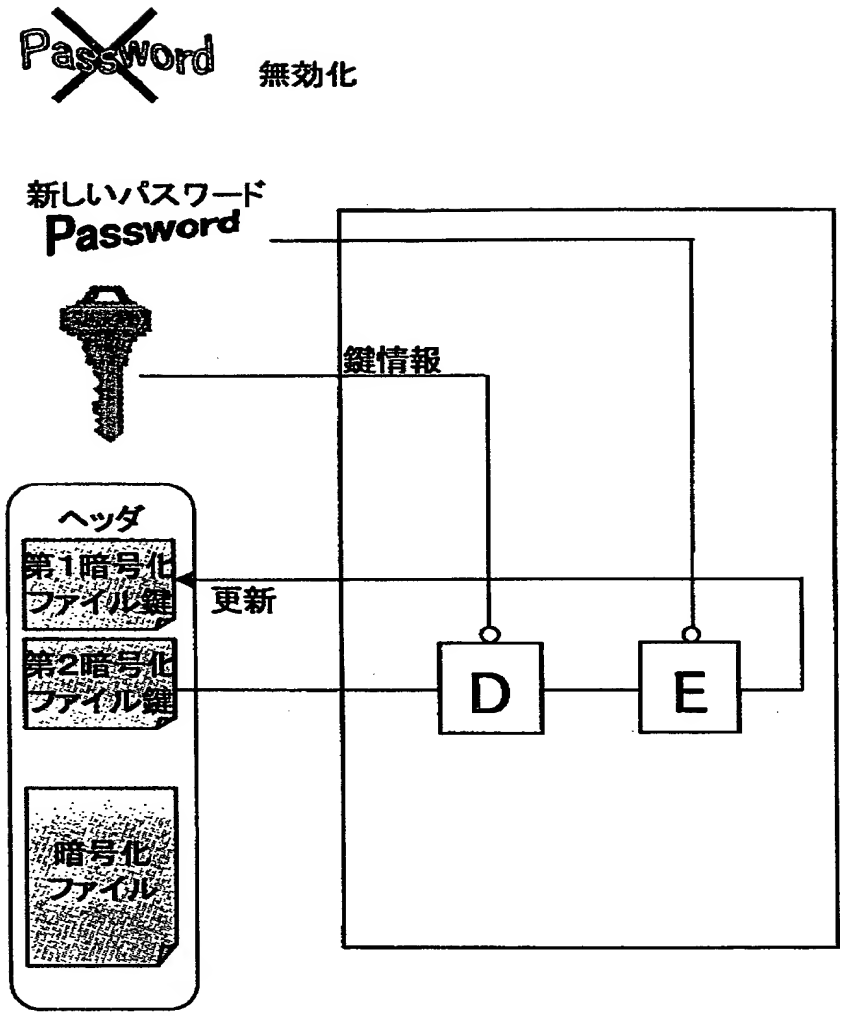
【図７】


暗号化パスワード
D
パスワード
E
ヘッダ
鍵情報
第1暗号化ファイル鍵
ファイル鍵
E
第2暗号化ファイル鍵
ファイル
E
暗号化ファイル

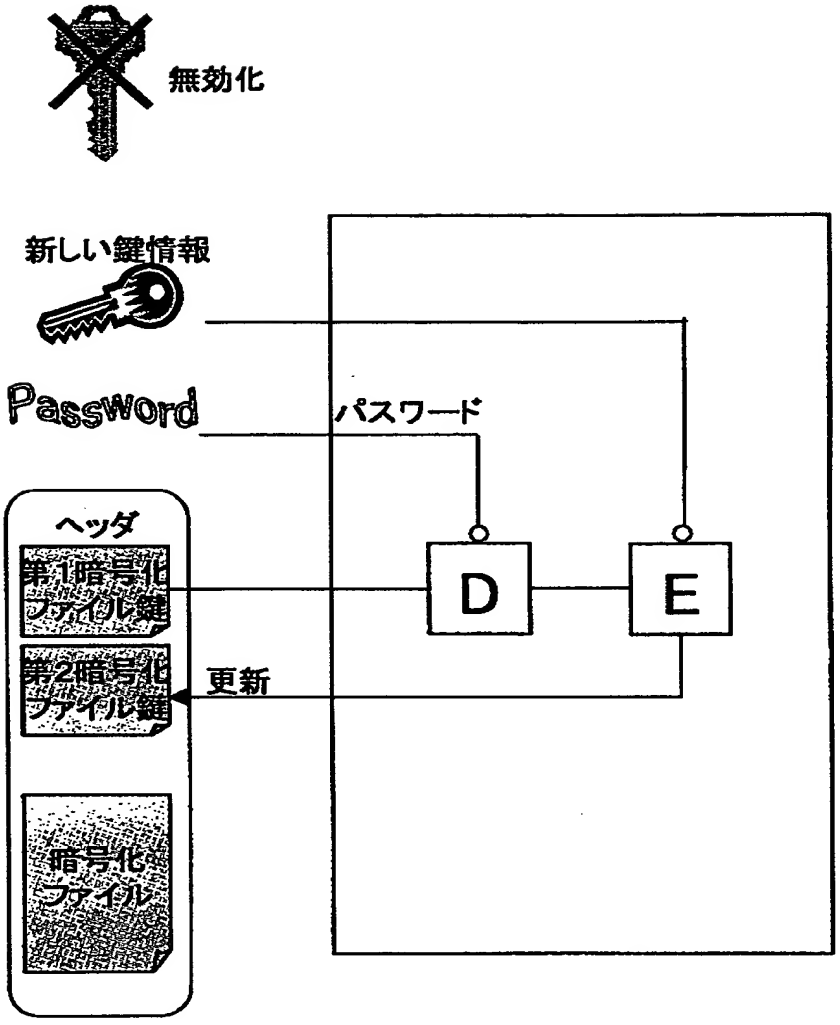
【図８】


ファイル
D
D
パスワード
PassWord
ヘッダ
第1暗号化ファイル鍵
第2暗号化ファイル鍵
暗号化ファイル
(b)
ファイル
D
D
鍵情報
ヘッダ
第1暗号化ファイル鍵
第2暗号化ファイル鍵
暗号化ファイル
(a)

【図９】


Password
無効化
新しいパスワード
Password
鍵情報
ヘッダ
第1暗号化ファイル鍵
更新
第2暗号化ファイル鍵
暗号化ファイル
D
E

【図１０】


無効化
新しい鍵情報
Password
パスワード
ヘッダ
第1暗号化ファイル鍵
第2暗号化ファイル鍵
暗号化ファイル
D
E
更新

【書類名】　要約書

【要約】

【課題】　計算機に付随した鍵情報とパスワードを用いて、安全性が高く、ユーザに使いやすいファイル暗号復号システムを実現する。

【解決手段】　計算機に付随した鍵情報を用いてファイルの暗号化と復号を行なう。加えて、鍵情報を用いてあらかじめパスワードを登録し、暗号化鍵、あるいは暗号化パスワードを格納する。この情報を用いて、パスワードだけで復号が可能になる。また、鍵情報を紛失したときに、鍵情報を一時的に無効化したり、新しい鍵情報が発行されたときにも、前の鍵情報で暗号化したファイルを扱えるための仕組みを備える。

【選択図】　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社